Ahmad Yousuf

Portfolio Project 1

06/21/2025

SIEM Log Analysis Lab Using Splunk

Objective

To design and implement a virtual lab environment leveraging Splunk for ingesting and analyzing Windows and firewall logs. The project focuses on building custom dashboards and correlation searches to detect simulated security threats.

Background and Motivation

Security Information and Event Management (SIEM) platforms are critical tools in modern cybersecurity operations. They enable centralized collection, normalization, and analysis of log data from various sources, allowing security teams to detect and respond to threats in real time. Splunk is a widely adopted SIEM solution known for its scalability and powerful search capabilities. This project aims to provide hands-on experience with Splunk in a controlled lab setting, simulating real-world log ingestion and threat detection workflows.

Scope

The scope of this project includes:

- Setting up a virtual lab environment with Splunk.
- Ingesting logs from Windows systems and a firewall device.
- Creating dashboards to visualize log data.
- Developing correlation searches to identify simulated threats.
- The project is limited to log ingestion, dashboard creation, and basic threat detection within a virtual lab.

Tools and Technologies

- Splunk Enterprise (trial version)
- Splunk Universal Forwarder
- Windows 10 or Windows Server (virtual machine)

- pfSense firewall (virtual machine)
- Sysmon (Windows system monitoring tool)
- VirtualBox or VMware Workstation
- Syslog protocol for firewall log forwarding
- Basic scripting (PowerShell, Bash) for simulation

Implementation Steps

1. Lab Environment Setup

- Installed VirtualBox and created three virtual machines:
    - One running Splunk Enterprise.
    - One running Windows 10 with Sysmon installed.
    - One running pfSense as the firewall.
- Configured network interfaces to allow communication between all VMs.

2. Splunk Installation and Configuration

- Installed Splunk Enterprise on a dedicated VM.
- Configured Splunk to listen on TCP/UDP ports for incoming log data.
- Created indexes for Windows logs (windows_logs) and firewall logs (firewall_logs).

3. Windows Log Ingestion

- Installed Sysmon on the Windows VM to generate detailed system logs.
- Installed Splunk Universal Forwarder on the Windows VM.
- Configured inputs.conf to monitor Sysmon log files and Windows Event Logs.
- Configured outputs.conf to forward logs to the Splunk server.
- Verified successful ingestion by searching for Sysmon events in Splunk.

4. Firewall Log Ingestion

- Configured pfSense to forward logs via syslog to the Splunk server.
- Created a new data input in Splunk to receive syslog messages.
- Defined a custom sourcetype for pfSense logs to facilitate field extraction.

- Verified log ingestion by searching for firewall events in Splunk.

5. Data Normalization and Field Extraction

- Used Splunk's Field Extractor to define custom fields for Sysmon and pfSense logs.
- Applied regular expressions to extract IP addresses, ports, usernames, and event types.
- Tagged and aliased fields to align with Splunk's Common Information Model (CIM).

6. Dashboard Development

- Created a dashboard for Windows logs showing:
    - Login attempts (successful and failed).
    - Process creation events.
    - Registry modifications.
- Created a dashboard for firewall logs showing:
    - Allowed and blocked traffic.
    - Source and destination IPs.
    - Port activity over time.

7. Correlation Searches and Threat Simulation

- Simulated brute force login attempts using PowerShell scripts on the Windows VM.
- Simulated port scanning activity targeting the pfSense firewall.
- Developed correlation searches to detect:
    - Multiple failed login attempts from a single IP within a short time window.
    - High volume of traffic to sequential ports from a single source.
- Configured alerts to trigger when correlation conditions were met.

Challenges and Solutions

- **Log Format Inconsistency**: Addressed by creating custom sourcetypes and field extractions.

- **Firewall Log Noise**: Filtered out non-essential events using Splunk search filters.
- **Simulated Threat Accuracy**: Ensured realistic simulation by scripting events with appropriate timing and volume.

Security Considerations

- Ensured secure communication between forwarders and Splunk using SSL.
- Restricted access to Splunk management interface with strong credentials.
- Isolated the lab environment from external networks to prevent unintended exposure.

Results and Evaluation

- Successfully ingested and parsed logs from both Windows and firewall sources.
- Dashboards provided clear visibility into system and network activity.
- Correlation searches accurately detected simulated threats with minimal false positives.
- Alerts were triggered as expected, demonstrating effective threat detection logic.

Future Improvements

- Expand log sources to include Linux systems and cloud services.
- Integrate Splunk Enterprise Security for advanced analytics.
- Implement machine learning-based anomaly detection models.
- Automate threat simulation using tools like Caldera or Atomic Red Team.

Conclusion

This project provided practical experience in deploying and configuring a SIEM solution using Splunk. It demonstrated the end-to-end workflow of log ingestion, normalization, visualization, and threat detection in a controlled lab environment. The skills developed are directly applicable to real-world security operations and incident response.

References and Resources

- Splunk Documentation: https://docs.splunk.com
- Sysmon: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
- pfSense Documentation: https://docs.netgate.com/pfsense/en/latest/

- Splunk Security Use Cases: https://www.splunk.com/en_us/solutions/security.html